

Cisco Unified Intelligence Center (CUIC) のための Citrix NetScaler 負荷つりあい機設定

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[HTTP/HTTPS の Unified Intelligence Center レポートにアクセスして下さい](#)

[設定](#)

[システム設定](#)

[アップロード ライセンス](#)

[ネットワーク構成](#)

[サブネット IP を作成して下さい](#)

[VIP を作成して下さい](#)

[ルーティングを作成して下さい](#)

[HTTPS ロード バランシング 設定](#)

[監視を作成して下さい](#)

[http ポート 80 のためのモニタを作成して下さい](#)

[サーバを作成して下さい](#)

[サービスを作成して下さい](#)

[仮想サーバの作成](#)

[持続グループを作成して下さい](#)

[参考資料](#)

概要

この資料は CUIC のために Citrix NetScaler 負荷 balancer を使用するためにコンフィギュレーションのステップを記述したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- CUIC
- Citrix Netscaler

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

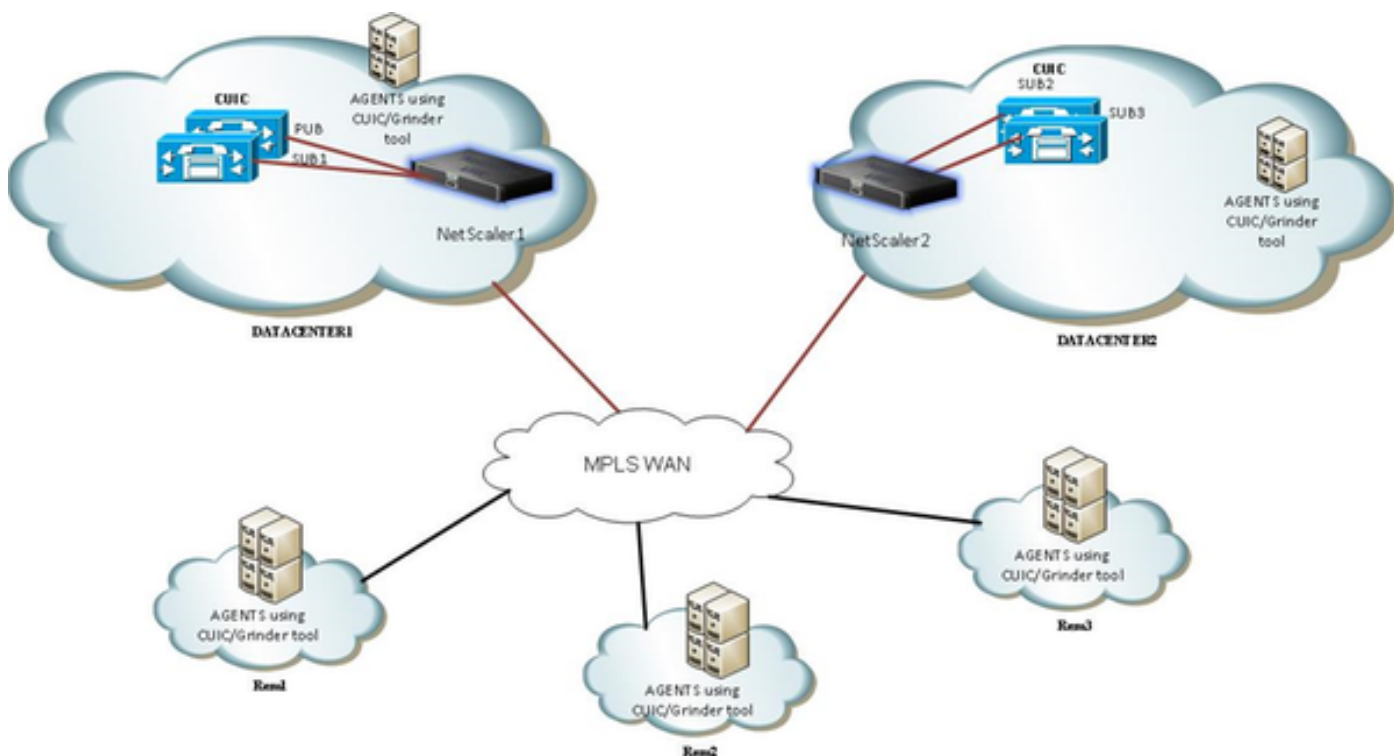
- CUIC 11.0(1)
- Citrix NS: アプライアンス 版: Citrix NetScaler 1000v (125.8) 10.1 ビルド

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

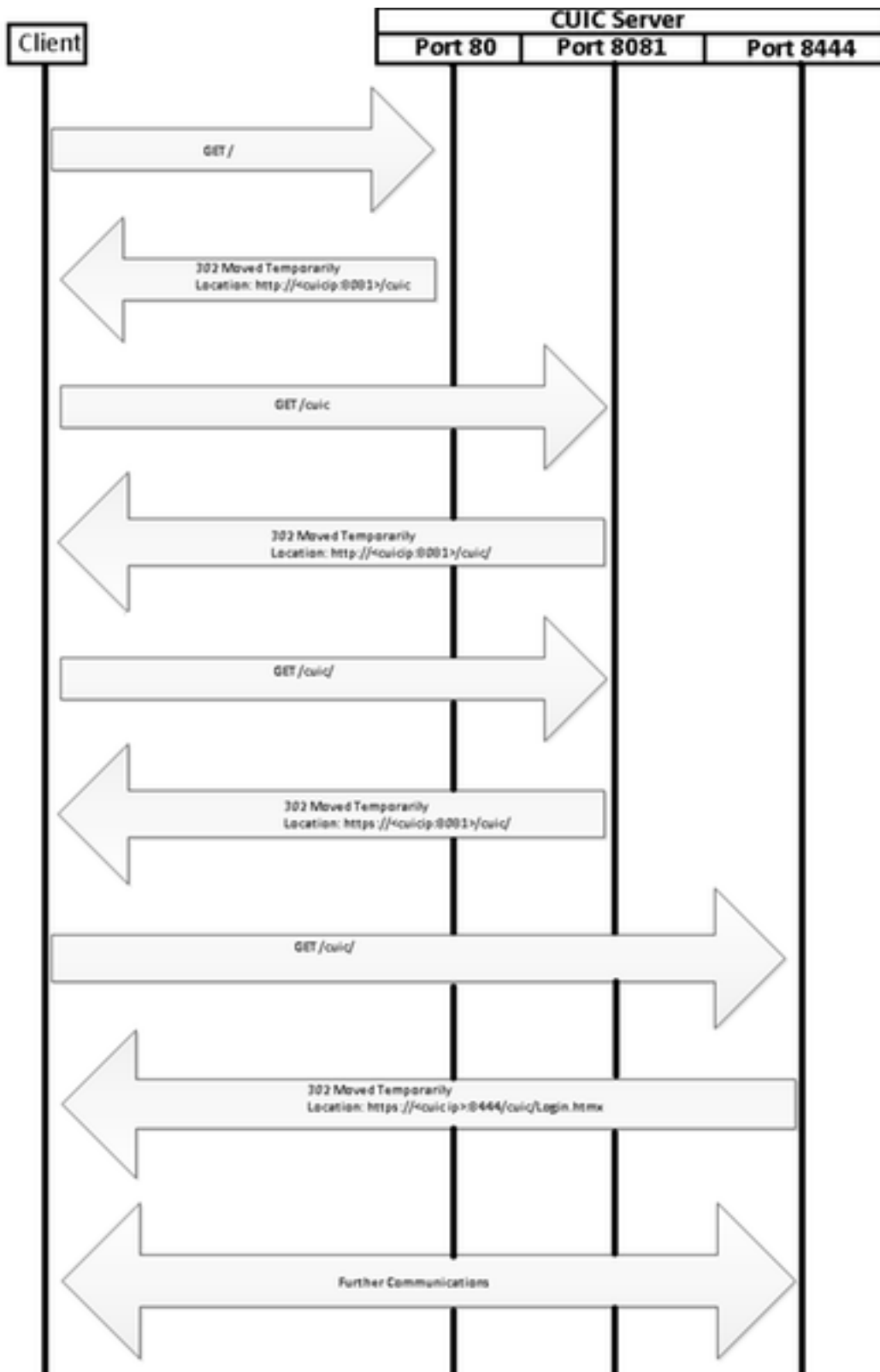
CUIC は関連した仕事上のデータでレポートを与える適用範囲が広く、直観的な Web ベース レポート プラットフォームです。CUIC を使うと、コンタクトセンター レポート および ダッシュボードが組織全体で共有され、共有される広範囲な情報ポータルを作成できます。大きい CUIC 配備では、Citrix NetScaler 1000v（負荷つりあい機）はロード バランス CUIC ハイパーテキスト転送プロトコル（HTTP）に使用され、Hypertext Transfer Protocol（HTTP）（HTTPS）トラフィックを保護します。

ネットワーク図



HTTP/HTTPS の Unified Intelligence Center レポートにアクセスして下さい

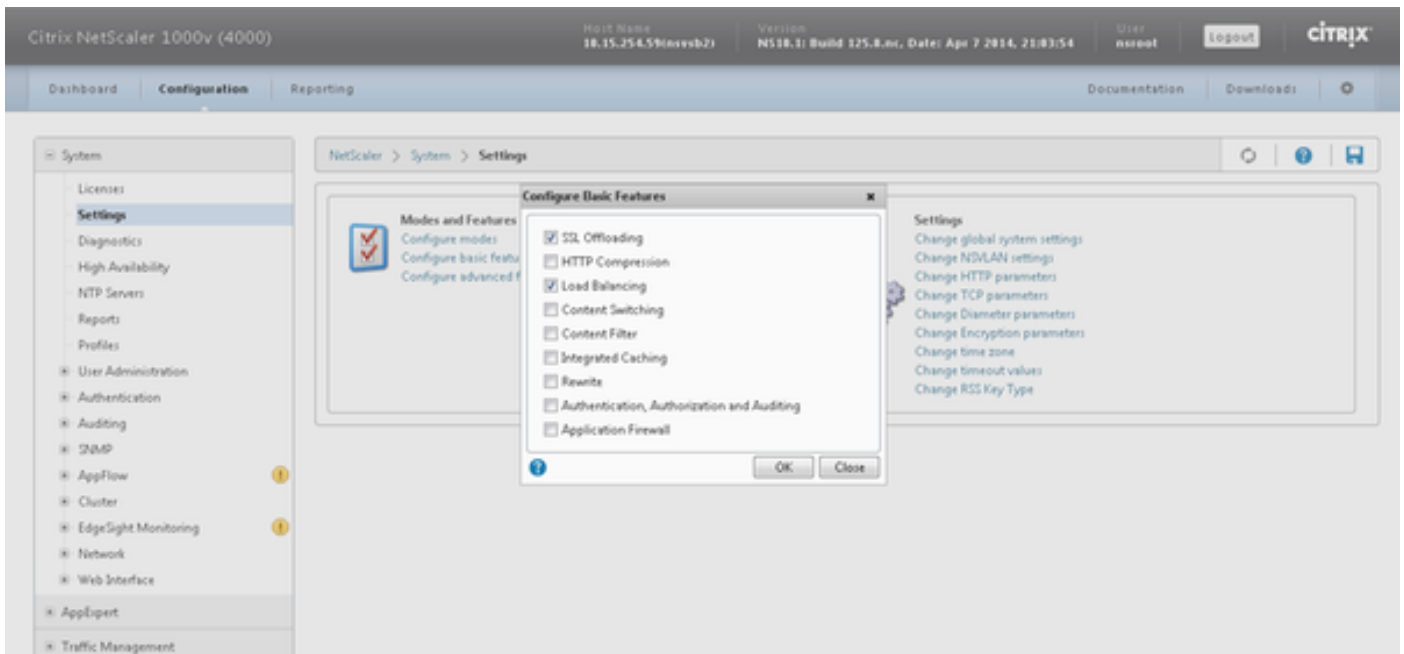
HTTP が CUIC サーバで無効になるとき、これは異なるポートへ HTTP フローです。



設定

システム設定

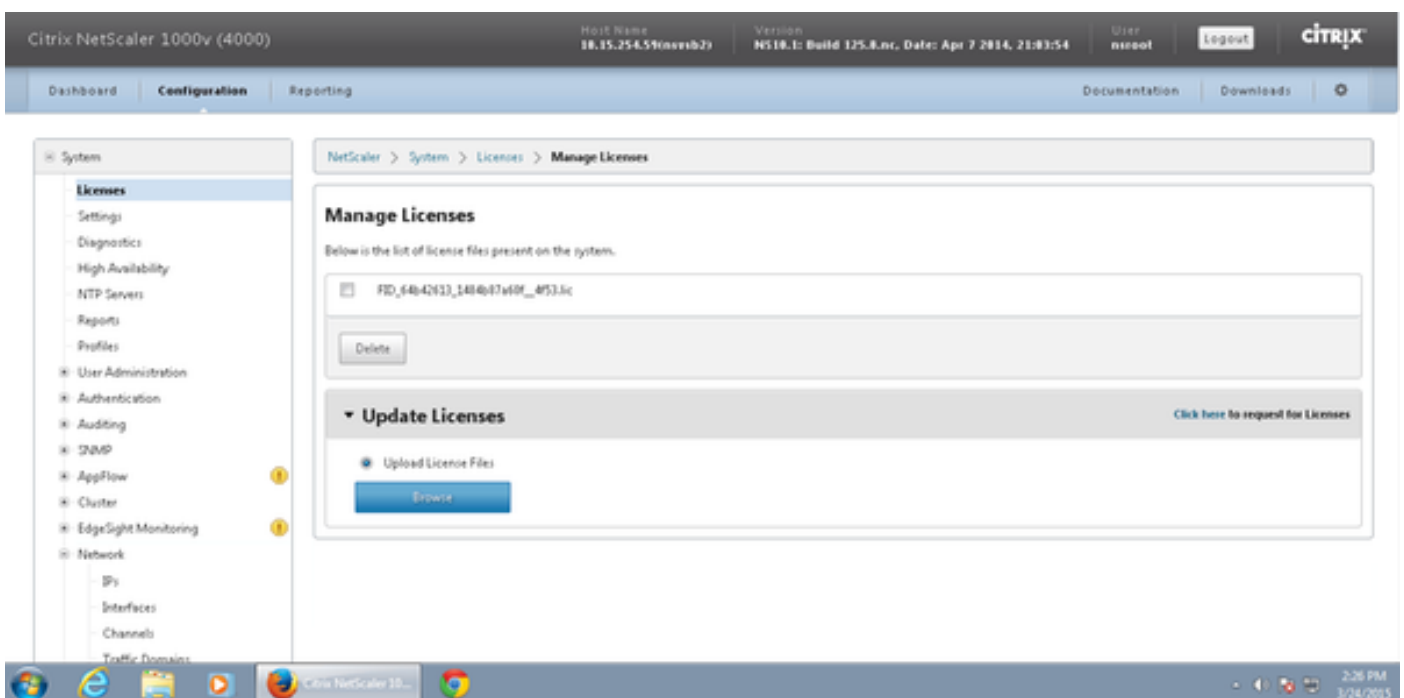
設定 > 設定 > 設定 基本的な機能



アップロード ライセンス

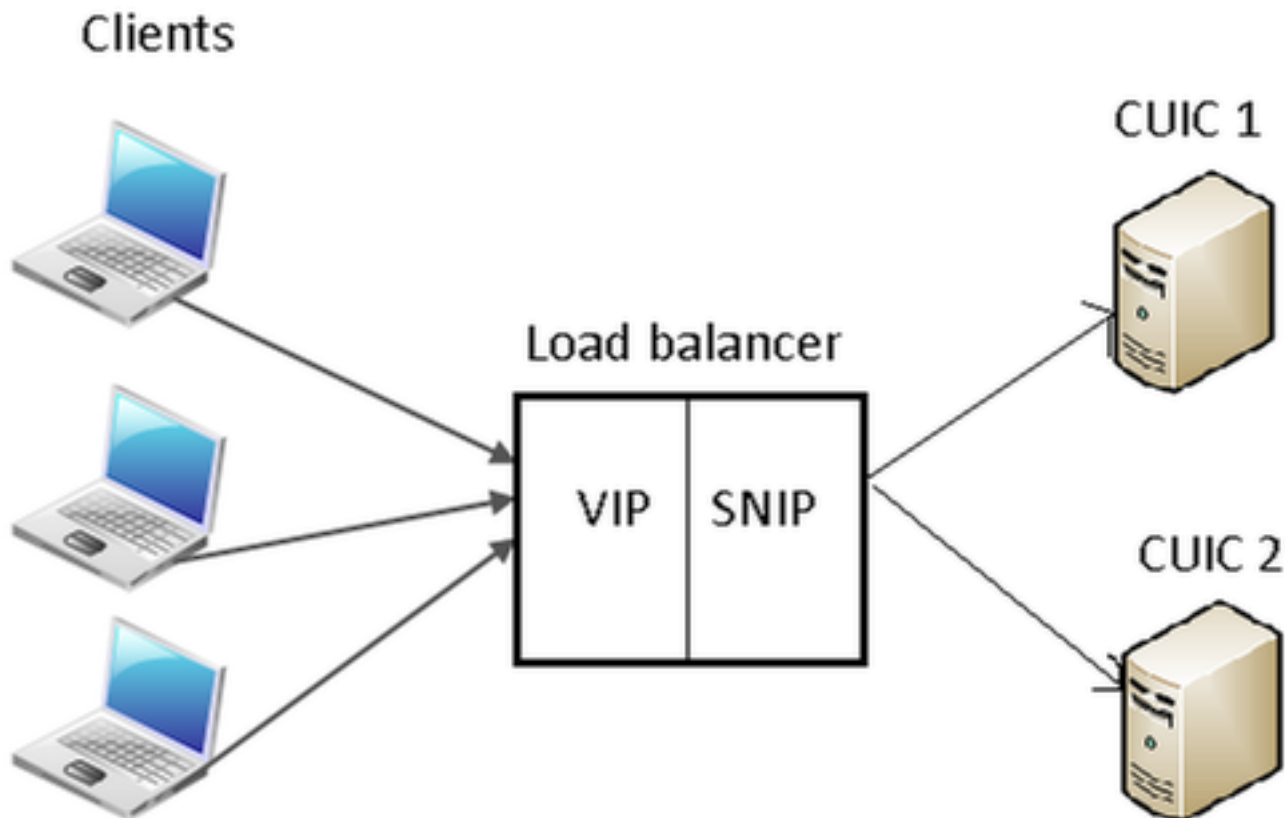
ライセンスなしで SSL ははたらかないかもしれません。

システム > ライセンスへの移動は > ライセンス > アップデート ライセンスを管理します



ネットワーク設定

クライアントはつりあい機を Virtual IP (VIP) によってロードし、サブネット IP (スニップ) を通して CUIC につりあい機話をロードするために話します。



システム > ネットワーク > IP > IPv4s をクリックして下さい

NetScaler > System > Network > IPs > IPv4s

IPv4s IPv6s

Add... Open... Remove Action Search

IP Address	Traffic Domain ID	State	Type	Mode	ARP	ICMP	Virtual Server
10.15.254.59	0	Enabled	NetScaler IP	Active	ENABLED	ENABLED	-N/A-
10.10.2.58	0	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
10.10.2.61	0	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED

25 Per Page 1 - 3 of 3 1

サブネット IP を作成して下さい

ステップ 1. IP アドレスを追加するために『Add』 をクリックして下さいサブネット IP として『Type』 を選択して下さい。

ステップ 2. 所望のIPアドレスを作成するために『Create』 をクリックして下さい。

Configure IP

IP Address	<input type="text" value="10 . 10 . 2 . 58"/>	Netmask	<input type="text" value="255 . 255 . 255 . 0"/>
Type	<input type="text" value="Subnet IP"/>	Mode	<input type="text" value="Active"/>
Virtual Router ID	<input type="text"/>	ICMP Response*	<input type="text" value="NONE"/>
ARP Response*	<input type="text" value="NONE"/>	Traffic Domain ID	<input type="text"/>

Options

ARP
 ICMP
 Virtual Server
 Dynamic Routing

Host Route

Enable

Gateway IP Metric

OSPF LSA Type

TYPE5
 TYPE1
Area

Vserver RHI Level

NONE
 ONE_VSERVER
 ALL_VSERVERS

Application Access Controls

Enable Management Access control to support the below listed applications.

VIP を作成して下さい

ステップ 1. IP アドレスを追加するために『Add』 をクリックして下さい。『バーチャルIP』として『Type』を選択して下さい。

ステップ 2. 所望のIPアドレスを作成するために『Create』 をクリックして下さい。

Configure IP

IP Address	<input type="text" value="10 . 10 . 2 . 61"/>	Netmask	<input type="text" value="255 . 255 . 255 . 255"/>
Type	<input type="text" value="Virtual IP"/>	Mode	<input type="text" value="Active"/>
Virtual Router ID	<input type="text"/>	ICMP Response*	<input type="text" value="NONE"/>
ARP Response*	<input type="text" value="NONE"/>	Traffic Domain ID	<input type="text"/>

Options

ARP
 ICMP
 Virtual Server
 Dynamic Routing

Host Route

Enable

Gateway IP Metric

OSPF LSA Type

TYPE5
 TYPE1
Area

Vserver RHI Level

NONE
 ONE_VSERVER
 ALL_VSERVERS

Application Access Controls

Enable Management Access control to support the below listed applications.

ルーティングを作成して下さい

もし必要なら、からの HTTP/HTTPS 要求が つりあい機 をロードすることを 来る ネットワーク にルーティングを作成して下さい。

Configure Route

Network: 10 . 3 . 4 . 0

Netmask: 255 . 255 . 255 . 0

Traffic Domain ID: [dropdown]

NULL Route: Yes No

Gateway: 10 . 10 . 2 . 1

Distance: 1

Weight: 1

Cost: 0

Route Advertisement

Global State DISABLED

Over-ride Global

Protocol

OSPF RIP BGP ISIS

Monitored Static Route

Buttons: [?] [Create] [Close]

望ましいルートを作成するために『Create』をクリックして下さい。

HTTPS ロード バランシング 設定

仮想サーバ エントリを、CUIC の各ポートのための 1 つは作成するために、3 つのポート監視される必要があります (HTTP ポート 80。 8081 および 8444) HTTPS ポート。各仮想サーバ エントリはクライアントから HTTP トラフィックを受信する IP およびポートの組み合わせです (CUIC レポートにアクセスしている)。

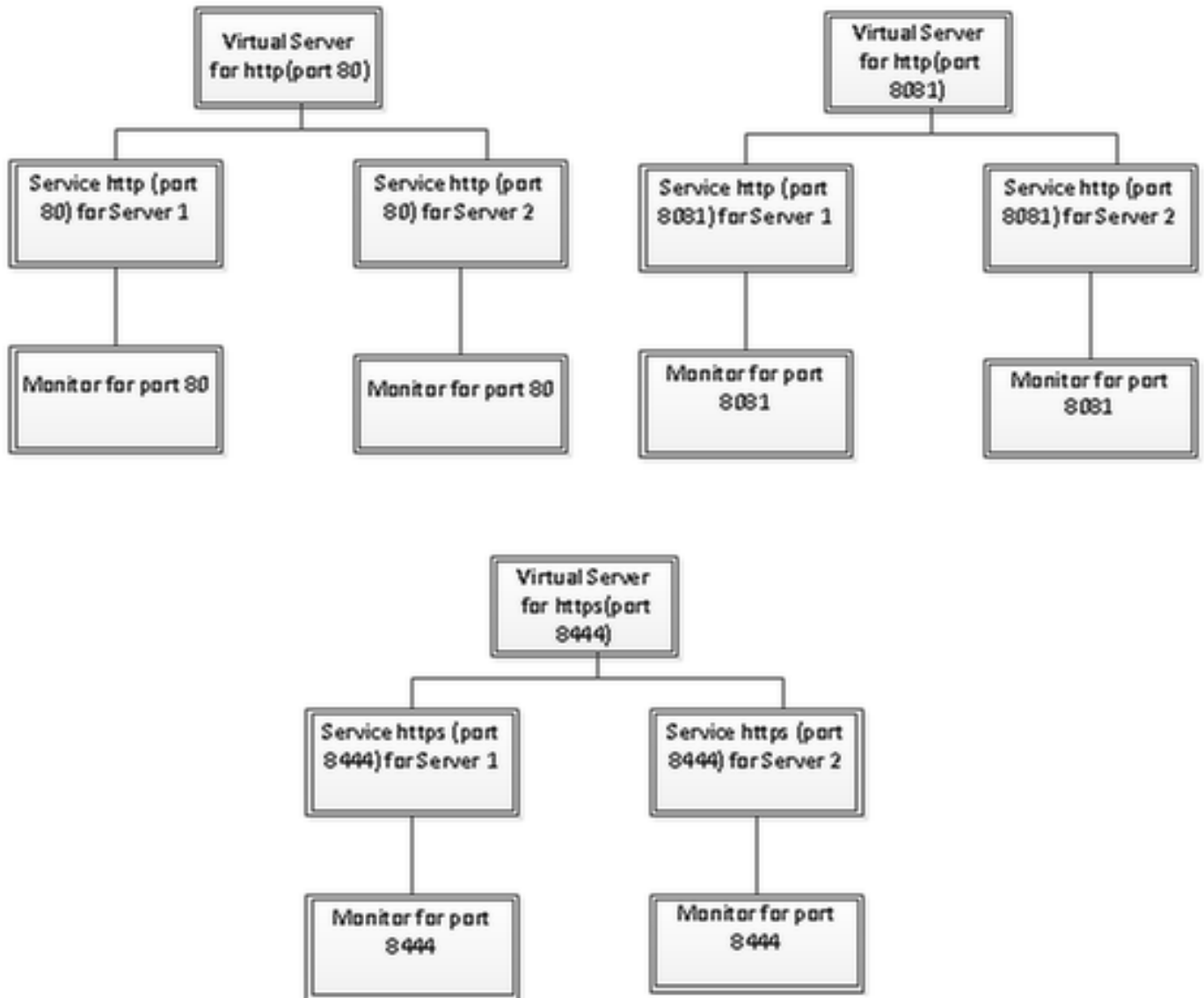
仮想サーバが負荷トラフィックを送信するためにそれらサーバによってリンクされるように必要となります。サーバの監視のヘルス ステータスをチェックするために、それらは各サーバに割り当てられる必要があります。監視を使用する、負荷はサーバ (CUIC) 失敗を検知し、要求を動作する健康にあるサーバに着信トラフィックを再配布します。

従ってアソシエーションはバーチャル Server->Service および Server->Monitor です。

設定の要約:

- 監視を作成して下さい
- サーバを作成して下さい
- サーバアソシエーションでサービスを作成して下さい
- 対応する監視に各サービスをリンクして下さい
- 仮想サーバを作成して下さい
- 仮想サーバと対応したサービスをリンクして下さい
- 持続グループを作成し、仮想サーバを追加して下さい

このイメージは3つの仮想サーバエントリおよびアソシエーションを描写します。



監視を作成して下さい

トラフィック管理 > ロード バランシング > 監視にナビゲートして下さい

NetScaler > Traffic Management > Load Balancing > Monitors

Name	State	Type
ping-default	Enabled	PING
tcp-default	Enabled	TCP
arp	Enabled	ARP
nd6	Enabled	ND6
ping	Enabled	PING
tcp	Enabled	TCP

モニタを作成するために、トラフィック管理 > ロード バランシング > モニタに、『Add』 をクリックします ボタンをナビゲートして下さい。

監視の 3 つの型は、ポート 80 のために、8081and 8444 作成されます。

http ポート 80 のためのモニタを作成して下さい

TCP として『Type』 を選択し、間隔、応答タイムアウト、ダウンタイム、再試行等をそれに
 じて規定して下さい。

モニタを作成するために『Create』 をクリックして下さい。HTTPS に関しては、作成される 2
 つの監視必要 (サーバごとに 1 つ)。

Create Monitor

Name* Type*

Standard Parameters | Special Parameters

Interval Minutes IPv6

Response Time-out Seconds

Down Time Seconds

Deviation Seconds

Retries Resp Time-out Threshold

SNMP Alert Retries Action

Success Retries Custom Header

Failure Retries Treat back slash as escape character

Enabled Reverse

LRTM (Least Response Time using Monitoring) Transparent Secure IP Tunnel

TOS TOSId

Create Monitor [X]

Name* Type* HTTP

Standard Parameters | Special Parameters

Interval Destination IP IPv6

Response Time-out Destination Port

Down Time Dynamic Time-out

Deviation Dynamic Interval

Retries Resp Time-out Threshold

SNMP Alert Retries Action

Success Retries Custom Header

Failure Retries Treat back slash as escape character

Enabled Reverse

LRTM (Least Response Time using Monitoring)

TOS TOSId Net Profile

Transparent Secure IP Tunnel

Help

HTTPS 型モニタに関しては、特別なパラメータ セクションを設定して下さい。HTTP 要求への応答が 200 または 302 である場合この Monitor レポート成功。

HTTP が CUIC で無効になるとき、302 は別の方法で 200 期待されます。両方の状況 200 および 302 を取扱うために含まれていて下さい。

Configure Monitor

Name* Type HTTP

Standard Parameters | Special Parameters

HTTP Request

Treat back slash as escape character

Response Codes

Create Monitor

Name* Type* HTTP-ECV

Standard Parameters | Special Parameters

Interval Destination IP IPv6

Response Time-out Destination Port

Down Time Dynamic Time-out

Deviation Dynamic Interval

Retries Resp Time-out Threshold

SNMP Alert Retries Action

Success Retries Custom Header

Failure Retries Treat back slash as escape character

Enabled Reverse Net Profile

LRTM (Least Response Time using Monitoring) Transparent Secure IP Tunnel

TOS TOSId

HTTPS 型モニタに関しては、特別なパラメータ セクションを設定して下さい。応答がストリング稼働中が含まれているときだけこの Monitor レポート成功。

Configure Monitor ×

Name* Type HTTP-ECV

Standard Parameters | Special Parameters

Send String

Treat back slash as escape character

Receive String

Treat back slash as escape character

Create Monitor



Name*

Type*

Standard Parameters

Special Parameters

Interval

Response Time-out

Down Time

Deviation

Retries

SNMP Alert Retries

Success Retries

Failure Retries

Enabled Reverse

LRTM (Least Response Time using Monitoring)

TOS TOSId

Destination IP IPv6

Destination Port

Dynamic Time-out

Dynamic Interval

Resp Time-out Threshold

Action

Custom Header

Net Profile

Transparent

Secure IP Tunnel

Treat back slash as escape character

Help

Create

Close

Create Monitor [X]

Name* Type* HTTP-ECV

Standard Parameters | Special Parameters

Send String

Treat back slash as escape character

Receive String

Treat back slash as escape character

Help [?] Create Close

サーバを作成して下さい

サーバは CUIC ノードを表します。ロードつりあい機によって役立つ各 CUIC ノードに関しては Server エントリが必要となります。

NetScaler > Traffic Management > Load Balancing > Servers

Add... Open... Remove Action Search

Name	State	IPAddress / Domain	Traffic Domain ID
ATL-CUIC-SUB4	Enabled	10.10.2.46	0
ATL-CUIC-SUB5	Enabled	10.10.2.47	0

25 Per Page 1 - 2 of 2 1

サーバを作成するために、トラフィック管理 > ロード バランシング > サーバに、『Add』 をクリックします ボタンをナビゲートして下さい。

Create Server [Close]

Server Name*

IP Address Domain Name

IPAddress* IPv6

Traffic Domain ID

Translation IP Address

Translation Mask

Resolve Retry (secs)

IPv6 Domain

Enable after Creating

Comments

[?] [Create] [Close]

Create Server [Close]

Server Name*

IP Address Domain Name

IPAddress* IPv6

Traffic Domain ID

Translation IP Address

Translation Mask

Resolve Retry (secs)

IPv6 Domain

Enable after Creating

Comments

[?] [Create] [Close]

サービスを作成して下さい

モニタを作成するために、トラフィック管理 > ロード バランシング > Services に、『Add』をクリックしますナビゲートして下さい。

NetScaler > Traffic Management > Load Balancing > Services

Buttons: Add... Open... Remove Action Search

Name	State	IP Address/Domain Name	Traffic Domain ID	Port	Protocol	Max Clients	Max Requests	Cache Type
cuic-http80-sub4	Up	10.10.2.46	0	80	HTTP	0	0	SERVER
cuic-http80-sub5	Up	10.10.2.47	0	80	HTTP	0	0	SERVER
cuic-http80801-sub4	Up	10.10.2.46	0	8081	HTTP	0	0	SERVER
cuic-http80801-sub5	Up	10.10.2.47	0	8081	HTTP	0	0	SERVER
cuic-https-sub4	Up	10.10.2.46	0	8444	SSL_BRIDGE	0	0	SERVER
cuic-https-sub5	Up	10.10.2.47	0	8444	SSL_BRIDGE	0	0	SERVER

25 Per Page 1 - 6 of 6 1

関連付けられる監視がないときデフォルト モニタは設定されたボックスで表示されるかもしれませんが。それを取除くことなしで、正しいモニタを利用可能なリストからの利用可能な監視から（このイメージでそれは `cust_tcp` です）選択し、設定されたリストにそれを移動するために『Add』をクリックして下さい。[OK]をクリックします。このページは開くとき次の時間、『Monitor』を選択されるただ示します。デフォルト モニタは消えます。これはので起こります；サービスは監視されると関連付けられる常に必要があります。何も設定されない場合、負荷つりあい機はデフォルト 1 を提供しますが、ユーザが監視される選択するときつりあい機を奪取しますデフォルト モニタをロードします。

Configure Service

Service Name* Server*

Protocol* Port*

Traffic Domain

Service State UP

Enable Health Monitoring AppFlow Logging

Monitors Policies Profiles Advanced SSL Settings

Available

Monitors
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp

Configured

Monitors	Weight	State
cust_tcp	1	<input checked="" type="checkbox"/>

State: UP
Probes: 68341 Failed [Total: 5614 Current: 0]
Last Response: Success - TCP syn+ack received.
Response Time: 0.357 millisec

Comments

Configure Service

Service Name* Server*
Protocol* Port*
Traffic Domain

Service State UP Down Number of Active Clients

Enable Health Monitoring AppFlow Logging

Thresholds

Max Requests	<input type="text" value="0"/>	Max Bandwidth (kbits)	<input type="text" value="0"/>
Max Clients	<input type="text" value="0"/>	Monitor Threshold	<input type="text" value="0"/>

Idle Time-out (secs)

Client Server

Settings

Use Source IP Client Keep-Alive TCP Buffering Compression
 Client IP Header

Comments

Configure Service

Service Name* Server*
Protocol* Port*
Traffic Domain

Service State UP Number of Active Clients
 Enable Health Monitoring AppFlow Logging

- Monitors
- Policies
- Profiles
- Advanced
- SSL Settings

Available

Monitors
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp

Configured

Monitors	Weight	State
http_8081	1	<input checked="" type="checkbox"/>

State: UP
Probes: 68352 Failed [Total: 5630 Current: 0]
Last Response: Success - HTTP response code 302 received.
Response Time: 0.754 millisc

Comments

Help

Configure Service

Service Name* Server*
Protocol* Port*
Traffic Domain

Service State UP Down Number of Active Clients
 Enable Health Monitoring AppFlow Logging

Thresholds

Max Requests	<input type="text" value="0"/>	Max Bandwidth (kbits)	<input type="text" value="0"/>
Max Clients	<input type="text" value="0"/>	Monitor Threshold	<input type="text" value="0"/>

Idle Time-out (secs)

Client Server

Settings

Use Source IP Client Keep-Alive TCP Buffering Compression

Client IP Header

Comments

Configure Service



Service Name* Server*
Protocol* Port*
Traffic Domain

Service State UP DOWN Number of Active Clients
 Enable Health Monitoring AppFlow Logging

- Monitors
- Policies
- Profiles
- Advanced
- SSL Settings

Available

Monitors
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp

Configured

Monitors	Weight	State
cust_sub4_https-ecv	1	<input checked="" type="checkbox"/>

State: UP
Probes: 384901 Failed [Total: 8624 Current: 0]
Last Response: Success - Pattern found in response.
Response Time: 1.463 millisec

Comments

Help

Configure Service [X]

Service Name* Server*
 Protocol* Port*
 Traffic Domain

Service State UP DOWN Number of Active Clients

Enable Health Monitoring AppFlow Logging

Monitors | Policies | Profiles | **Advanced** | SSL Settings

Thresholds

Max Requests	<input type="text" value="0"/>	Max Bandwidth (kbits)	<input type="text" value="0"/>
Max Clients	<input type="text" value="0"/>	Monitor Threshold	<input type="text" value="0"/>

Idle Time-out (secs)

Client Server

Settings

Use Source IP Client Keep-Alive TCP Buffering Compression

Client IP Header

Comments

仮想サーバの作成

NetScaler > Traffic Management > Load Balancing > Virtual Servers

Name	State	Effective State	IP Address	Traffic Domain ID	Port	Protocol	Method	Persistence	% Health
▶ DC2-CUBC-HTTP	<input checked="" type="radio"/> Up	<input checked="" type="radio"/> Up	10.10.2.61	0	80	HTTP	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN
▶ DC2-CUBC-HTTP8081	<input checked="" type="radio"/> Up	<input checked="" type="radio"/> Up	10.10.2.61	0	8081	HTTP	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN
▶ DC2-CUBC-HTTPS	<input checked="" type="radio"/> Up	<input checked="" type="radio"/> Up	10.10.2.61	0	8444	SSL_BRIDGE	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN

25 Per Page | 1 - 3 of 3 | 1

仮想サーバを作成するために、トラフィック管理 > ロード バランシング > 仮想サーバにナビゲートし、『Add』 をクリックして下さい。

サービスをチェックして下さいこのバーチャル サービスと関連付けられる必要がある。

最少接続として方式および永続性タブ、選択メソッド、SOURCEIP として永続性および 40 分としてタイムアウト。これはデフォルト史的記事リフレッシュレートが 30 分に設定されるという理由によります; リフレッシュレートより大きい値を設定する必要があります。 史的記事のための別のリフレッシュレートを設定する場合、この値を同様に変更して下さい。

Configure Virtual Server (Load Balancing)

Name* IP Address Based IP Pattern Based

Protocol* HTTP IP Address* 10 . 10 . 2 . 61

Network VServer Range 1 Port* 80

Enable DNS64 Bypass AAAA Requests Traffic Domain ID

State UP Disable AppFlow Logging

Services | Service Groups | Policies | Method and Persistence | Advanced | Profiles | SSL Settings

LB Method

Method Least Connection New Service Startup Request Rate PER_SECOND

Increment Interval

Current Method: Round Robin
Reason: Bound service's state changed to UP

Persistence

Persistence SOURCEIP Time-out (min) 40

Backup Persistence

Persistence NONE Time-out (min) 2

IPv4 Netmask IPv6 Mask Length 128

Configure Virtual Server (Load Balancing)

Name* IP Address Based IP Pattern Based

Protocol* HTTP IP Address* 10 . 10 . 2 . 61

Network VServer Range 1 Port* 8081

Enable DNS64 Bypass AAAA Requests Traffic Domain ID

State UP Disable AppFlow Logging

Services | Service Groups | Policies | Method and Persistence | Advanced | Profiles | SSL Settings

[Activate All](#) [Deactivate All](#)

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight
<input checked="" type="checkbox"/>	cuic-http80801-sub4	10.10.2.46	8081	HTTP	<input checked="" type="radio"/> UP	1	0
<input checked="" type="checkbox"/>	cuic-http80801-sub5	10.10.2.47	8081	HTTP	<input checked="" type="radio"/> UP	1	0
<input type="checkbox"/>	cuic-http80-sub4	10.10.2.46	80	HTTP	<input checked="" type="radio"/> UP	1	
<input type="checkbox"/>	cuic-http80-sub5	10.10.2.47	80	HTTP	<input checked="" type="radio"/> UP	1	

Comments

Configure Virtual Server (Load Balancing)

Name* IP Address Based IP Pattern Based

Protocol* IP Address*

Network VServer Range Port*

Enable DNS64 Bypass AAAA Requests Traffic Domain ID

State UP AppFlow Logging

Services | Service Groups | Policies | Method and Persistence | Advanced | Profiles | SSL Settings

[Activate All](#) [Deactivate All](#)

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight
<input checked="" type="checkbox"/>	cuic-https-sub4	10.10.2.46	8444	SSL_BRIDGE	<input checked="" type="radio"/> UP	<input type="text" value="1"/>	0
<input checked="" type="checkbox"/>	cuic-https-sub5	10.10.2.47	8444	SSL_BRIDGE	<input checked="" type="radio"/> UP	<input type="text" value="1"/>	0

Comments

持続グループを作成して下さい

持続グループを作成するために、トラフィック管理 > ロード バランシング > 持続グループに、『Add』をクリックしますナビゲートして下さい。

最少接続として選択メソッド、SOURCEIPとして永続性および40分としてタイムアウト。これはデフォルト史的記事リフレッシュレートが30分に設定されるという理由によります;リフレッシュレートより大きい値を設定する必要があります。 史的記事のための別のリフレッシュレートを設定する場合、この値を同様に変更して下さい。

各CUICサーバが3つのポートで受信するので、3つの仮想サーバをすべてここに含む必要があります。Client要求が同じCUICに特定のCUICサーバに既に送信されているHTTP80ポートに、ポート8081に目標としていればそのクライアントからのすべての要求8444ルーティングされれば。

Configure Persistency Group

Group Name: PgroupDC2

Persistence*: SOURCEIP

IPv4 Netmask: 255 . 255 . 255 . 255

IPv6 Mask Length: 128

Time-out: 40

Backup Persistence*: NONE

Virtual Server Name*

Configured (3) Remove All

DC2-CUIC-HTTP	-
DC2-CUIC-HTTP8081	-
DC2-CUIC-HTTPS	-

+ Add

? OK Close

参照

1. <http://support.citrix.com/proddocs/topic/netScaler/ns-gen-netScaler-wrapper-con.html>